PECB Certified ISO/IEC 27005 Lead Risk Manager

Master the fundamental principles and concepts of Risk Assessment and Optimal Risk Management in Information Security based on ISO/IEC 27005:2022.

Why should you attend?

ISO/IEC 27005:2022 Lead Risk Manager training enables you to develop the competence to master the risk management process related to all assets of relevance for Information Security using the ISO/IEC 27005:2022 standard as a reference framework. During this training course, you will gain a comprehensive knowledge of a process model for designing and developing an Information Security Risk Management program. The training will also contain a thorough understanding of best practices of risk assessment methods such as OCTAVE, EBIOS, MEHARI and harmonized TRA. This training course supports the implementation process of the ISMS framework presented in the ISO/IEC 27001 standard.

After mastering all the necessary concepts of Information Security Risk Management based on ISO/IEC 27005:2022, you can sit for the exam and apply for a "PECB Certified ISO/IEC 27005:2022 Lead Risk Manager" credential. By holding a PECB Lead Risk Manager Certificate, you will be able to demonstrate that you have the practical knowledge and professional capabilities to support and lead a team in managing Information Security Risks.

Who should attend?

- Managers or consultants involved in or responsible for information security in an organization
- Individuals responsible for managing information security risks, such as ISMS professionals and risk owners
- Members of information security teams, IT professionals, and privacy officers
- Individuals responsible for maintaining conformity with the information security requirements of ISO/IEC 27001 in an organization
- Project managers, consultants, or expert advisers seeking to master the management of information security risks

The main requirements for participating in this training course are having a fundamental understanding of ISO/IEC 27005 and comprehensive knowledge of risk management and information security.

COURSE DURATION	EXAM	EXAM DURATION	EXAM RETAKE
5 days	✔	3 hours	free

t

Learning objectives

- Understand the concepts, approaches, methods and techniques that enable an effective risk management process according to ISO/IEC 27005:2022
- Acknowledge the correlation between Information Security risk management and security controls
- Learn how to interpret the requirements of ISO/IEC 27001 in Information Security Risk Management
- Acquire the competence and skills to effectively advise organizations on Information Security Risk Management best practices
- Acquire the knowledge necessary for the implementation, management and maintenance of an ongoing risk management program

Course agenda

DAY 1   Introduction to ISO/IEC 27005:2022, concepts and implementation of a risk management program

Course objectives and structure • Standard and regulatory framework • Concepts and definitions of risk • Implementing a risk management programme • Context establishment

DAY 2   Risk identification, evaluation, and treatment as specified in ISO/IEC 27005:2022

Risk Identification • Risk Analysis • Risk Evaluation • Risk Assessment with a quantitative method • Risk Treatment

DAY 3   Information Security Risk Acceptance, Communication, Consultation, Monitoring and Review

Information security risk acceptance • Information security risk communication and consultation • Information security risk monitoring and review

DEN 4   Risk Assessment Methodologies

OCTAVE Method • MEHARI Method • EBIOS Method • Harmonized Threat and Risk Assessment (TRA) Method • Applying for certification and closing the training

DAY 5   Certification Exam

Training materials

The participant will receive training materials containing more than 400 pages of information and practical examples in electronic form via the KATE application. As part of the full-time course, the participant will also receive training materials in printed form.

Examination

The "PECB Certified ISO/IEC 27005:2022 Lead Risk Manager" exam fully meets the requirements of the PECB Examination and Certification Programme (ECP). The exam covers the following competency domains:

DOMAIN 1	Fundamental principles and concepts of Information Security Risk Management
DOMAIN 2	Implementation of an Information Security Risk Management program
DOMAIN 3	Information security risk assessment
DOMAIN 4	Information security risk treatment
DOMAIN 5	Information security risk communication, monitoring and improvement
DOMAIN 6	Information security risk assessment methodologies

The exam consists of 80 multiple-choice test questions (a, b, c) and is open book, i.e. it is possible to use reference materials such as a copy of the ISO standard, PECB training materials, personal notes from the course or a printed language dictionary. The exam lasts 3 hours and can be taken online or in person. If you do not pass the exam, you can retake it for free within 12 months.

Certification

Credential	Exam	Professional experience	Project experience
PECB Certified ISO/IEC 27005 Provisional Lead Risk Manager	PECB Certified ISO/IEC 27005 Lead Risk Manager	None	None
PECB Certified ISO/IEC 27005 Lead Risk Manager	PECB Certified ISO/IEC 27005 Lead Risk Manager	5 years: 2 years of experience in ISRM	Project activities: a total of 300 hours
PECB Certified ISO/IEC 27005 Senior Lead Risk Manager	PECB Certified ISO/IEC 27005 Lead Risk Manager	10 years: 7 years of experience in ISRM	Project activities: a total of 1 000 hours